CPNI Compliance Policies of Gamewood Technology Group, Inc.

Gamewood Technology Group, Inc. ("Company") has implemented the following policies and procedures to protect the confidentiality of Customer Proprietary Network Information ("CPNI") and to assure compliance with the rules of the Federal Communications Commission ("FCC") set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 et seq.

CPNI is "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."

Company primarily provides wholesale services and support for interconnected voice-over-IP service providers and other entities. For these services, Company has knowledge of end user CPNI only insofar as it is necessary for the provision and maintenance of service to its wholesale customers. Company also provides certain retail services to enterprise customers. The following summary describes Company's policies, administered by its CPNI Compliance Manager (M. Edward Wilborne, III), that is designed to protect the confidentiality of its customers' CPNI.

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

Company will use, disclose, or permit access to CPNI only in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including the publishing of directories; to initiate, render, bill and collect for telecommunications services; to protect its rights or property, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide inside wiring installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

Company does not use CPNI to market service offerings among the different categories of service, or even within the same category of service, that it provides to subscribers. Company does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

In accordance with Section 222(b) of the Act, 47 U.S.C. § 222(b), when Company receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it will only use such information for such purpose, and does not use such information for its own marketing efforts.

II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES

Above and beyond the specific FCC requirements, Company will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee becomes aware of possible new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to Company's existing policies that would strengthen protection of CPNI, they should report such information immediately to Company's CPNI Compliance Manager so that Company may evaluate whether existing policies should be supplemented or changed.

A. Inbound Calls to Company Requesting CPNI

Call Detail Information (CDI) is a subset of CPNI that includes any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

Company does not provide CDI to inbound callers. Company may send a copy of a bill or requested CDI to a mailing address of record for the account, but only if such address has been on file with Company for at least 30 days.

For CPNI other than CDI, CSRs are trained to require an inbound caller to authenticate their identity using methods appropriate for the information sought prior to revealing any CPNI or account information to the caller.

B. In-Person Disclosure of CPNI at Company Offices

Company may disclose a customer's CPNI to an authorized person visiting a Company office upon verifying that person's identity through a valid, non-expired government-issued photo ID (such as a driver's license, passport, or comparable ID) matching the customer's account information.

C. Notice of Account Changes

When an address of record is created or changed, except in connection with the customer's initiation of service, Company will immediately send a notice to customer's pre-existing address of record notifying them of the change. When an online account, password, and/or CPNI Authentication Passcode is created or changed, a notice will immediately be sent to customer's address of record notifying them of the change. Such notices will not reveal the changed information, and will direct the customer to notify its service provider immediately if they did not authorize the change.

D. Online Access to CPNI

When a customer submits a request for new telephone service, they must provide an email address that will serve as an address of record for their telephone account. An email is sent to the new customer's email address of record that includes a unique secure link that can be used to access on-line account through which the customer may obtain or update certain account information. The customer is initially authenticated through the use of this link. Upon initial entry into the on-line portal through this link, the customer is required to choose a password and a CPNI Authentication Passcode. After the user chooses a password, the authentication link sent to the customer expires and no longer provides entry into the account, which thereafter can only be accessed by correctly providing the login ID and password. The site instructs the user to select a password and Passcode that do not consist of any significant portion of the customer's name, family names, account number, telephone number, street address, zip code, social security number, date of birth, other biographical or account information, or easily guessed words or strings of digits. A password and/or the CPNI Authentication Passcode may be changed by the user after logging into the online account with the correct login ID and password. If a customer forgets their password, they may enter their CPNI Authentication Passcode to have their login credentials sent to their address of record. If they have also do not have their CPNI Authentication Passcode, they may only obtain these credentials by contacting company by phone and asking for these credentials to be

provided by a return telephone call to the telephone number of record for the account, or sent to the address of record that has been on file for 30 days, or they may visit a Company office and present photo identification that meets the requirements of Section II.B. herein. If there are 5 or more consecutive failed attempts at access to an online account without an intervening successful login, the account will be locked to protect it from serial access attempts by an unauthorized person. To unlock an account, the customer must call Company and provide identifying information to request that the account be unlocked. If there is an unusual number of requests to unlock an account, Company will contact the customer's telephone number of record or address of record to verify that the unlock requests were authorized by the customer.

E. Alternative Arrangements

Pursuant to 47 C.F.R. § 64.2010(g), the requirements set forth in this section III do not apply to business customer accounts (including Company's carrier customers) where the customer is able to contact a dedicated account representative and has a contract with Company that specifically addresses Company's protection of CPNI.

IV. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Any Company employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such information immediately to the Company CPNI Compliance Manager, and such information must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

It is Company's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate the Company's CPNI compliance procedures are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

A. Identifying a "Breach"

A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Manager.

If a Company employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to Company's CPNI Compliance Manager who will determine whether to report the incident to law enforcement and/or take other appropriate action. Company's Compliance Manager will determine whether it is appropriate to update Company's CPNI policies or training materials in light of any new information; the FCC's rules require Company on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting."

B. Notification Procedures

As soon as practicable, and in no event later than 7 business days upon learning of a breach, the Company CPNI Compliance Manager shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: https://www.cpnireporting.gov. Company's FRN number and password may be required to submit a report. If this link is not responsive, they should contact counsel or the FCC's Enforcement Bureau (202-418-7450 or http://www.fcc.gov/eb/cpni) for instructions.

Company will not notify customers or disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided below (a full business day does not count a business day on which the notice was provided). Federal law requires compliance with this requirement even if state law requires disclosure.

If Company receives no response from law enforcement after the 7th full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach.

Company will delay notification to customers or the public upon request of the FBI or USSS. If the Company Compliance Manager believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; Company still may not notify customers sooner unless given clearance to do so from both the USSS and the FBI.

V. RECORD RETENTION

The Company Compliance Manager is responsible for assuring that we maintain for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

Company maintains a record, for a period of at least one year, of those limited circumstances in which CPNI is disclosed or provided to third parties or where third parties were allowed access to CPNI. If Company later changes its policies to permit the use of CPNI for marketing, it will maintain a record, for at least one year, of supervisory review of marketing that proposes to use CPNI or to request customer approval to use or disclose CPNI.

An authorized corporate officer will sign a compliance certificate on an annual basis stating that the officer has personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC by March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how Company's operating procedures ensure compliance with the FCC's CPNI rules. In addition, the filing must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. Confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.

VI. TRAINING

All employees with access to CPNI receive a copy of Company's CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. In addition, Company conducts mandatory CPNI training for all CSRs, personnel at retail offices that may receive requests for CPNI, and marketing personnel. The CSR training emphasizes, among other points, that CSRs be cognizant that some unauthorized persons may have significant apparent familiarity with a customer's biographical and account information.